

M-12041US  
09/940,026**REMARKS**

Applicants respectfully traverse the interpretation of "storage engine" as reading on the clearing house of Hurtado (2003/0105718). However, to moot the issue, Applicants have amended claims 1 and 20 to recite a "media player." Support has been provided such as on page 11, lines 7-8.

Note the advantages of the media player recited in claim 20: the DRM (digital rights management) is controlled by the media player rather than a host. This is advantageous because hackers cannot obtain access to the workings of the media player as they would for a typical host such as a PC. As claimed, the host receives encrypted content from the media player. But the host has no control over access to the content key – that access is controlled by the media player. In contrast, the Hurtado reference is a conventional "host-based" DRM scheme. In that regard, the office action of 05-08-06 states that Hurtado discloses a block configured to transmit a session key to the host in paragraphs 18, 181, 185 and 206-215. But note that these paragraphs are directed to the generation at the clearing house (element 105) of a decryption key. See, e.g., paragraph 181. Indeed, consider the end user device in Hurtado (Figure 1D). As set forth in the abstract, this end user must establish a "secure connection with an authorization authority" to decrypt desired content. As such, this is a classic host-based DRM scheme. Whatever media player the Hurtado user device contains is entirely passive: just a disk reader. It in no way generates a random number, transmits the random number to a host, etc. Instead, it is the clearing house in Hurtado that generates the decryption key. In sharp contrast, it is the media player in claim 20 that generates the random number that enables a connected host device to decrypt content it is accessing through the media player. Not further that one cannot stretch the meaning of "media player" to include the clearing house of Hurtado because the Hurtado end user device/host does not receive encrypted content from this clearing house.

The Liu reference (USP 6,760,752) adds nothing further. The Liu reference is merely directed to secure transmission of data over a network (see, e.g., the abstract). Liu provides no teaching or suggestion to modify the conventional host-based DRM scheme in Hurtado into the advantageous storage-engine-based DRM provided by the storage engine of claim 20. Accordingly, claim 20 is patentable over the cited prior art.

M-12041US  
09/940,026

Claim 1 is patentable for analogous reasons. The cited prior art provides no suggestion or teaching for the inventive acts of “generating a random number at the media player and encrypting the random number with a public key extracted from the certificate to form a session key and transmitting the session key to the host” and “receiving an encrypted content key from the media player and decrypting the content key using the session key to recover the content key.” Given these acts, the flow of content from the media player to the host is enabled as recited by the acts of “at the media player, retrieving encrypted content from a media; transmitting the encrypted content to the host; and at the host, decrypting the encrypted content using the content key. As discussed above, the Hurtado reference is a conventional host-based scheme. There is no suggestion or teaching of a media player in Hurtado that generates a random number and encrypts the random number with a public key to form a session key and that transmits the session key to the host. Instead, all Hurtado discloses is a user device receiving decryption information through a secure connection to a clearing house. That is host-based and thus vulnerable to hacking scheme. In contrast, all the DRM “intelligence” recited in claim 1 is retained in the media player – a user has no access to this DRM capability and thus cannot hack it. Note further that content on the media is encrypted according to a content key. Thus, the host needs the content key to gain access to the content. However, for additional security, the media player does not simply provide the content key to the host. Instead, the content key is encrypted using the secure session key. Thus, the host can only recover the content key using the secure session key. As such, the secure session key is not a content key but rather is a key to the content key.


Thus, claim 1 and its dependent claims 2, 5-14, and 16-18 are thus patentable over the Hurtado and Liu references. Claim 20 is patentable for analogous reasons as discussed previously.

In addition, claim 1 has been amended to address the informality noted by the Examiner.

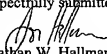
M-12041US  
09/940,026CONCLUSION

For the above reasons, claims 1, 2, 5 - 14, 16 - 18, and 20 are now in a condition for allowance. Applicant therefore respectfully requests that a timely Notice of Allowance be issued in this case.

If there are any questions regarding this amendment, the Examiner is invited to call the undersigned at (949) 752-7040.

Certification of Facsimile Transmission	
I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.	
 Jonathan Hallman	June 1, 2006 Date of Signature

Respectfully submitted,

  
Jonathan W. Hallman  
Attorney for Applicants  
Reg. No. 42,622  
Tel.: (949) 752-7040